REMARKS/ARGUMENTS

In the Final Office Action mailed March 30, 2004, claims 1-29 stand rejected. Applicants have thoroughly reviewed the outstanding Office Action including the Examiner's remarks and the references cited therein. The following remarks are believed to be fully responsive to the Final Office Action. All the pending claims at issue are believed to be patentable over the cited references.

CLAIM REJECTIONS – 35 U.S.C. § 103(a)

Claims 1-7, 11-17 and 21-29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Sasaki, et al. (U.S. Patent No. 6,134,488) and Chainer et al. (U.S. Patent No. 6,525,672). Applicants respectfully submit that the *Sasaki* and *Chainer* alone or in combination do not teach or suggest all the claim limitations of claims 1, 11, 24, 27, and their respective dependent claims.

Sasaki is directed to a diagnostic tool that forces an activation signal to a target portion of a vehicle being diagnosed. The diagnostic tool detects the current state of the target portion and compares the current state with a state predicted when the activation signal is sent to the target portion. A signal to stop a self diagnosis test for the target portion, which can vary due to the activation signal, is also sent to the vehicle. The diagnostic tool includes a ROM card 7 that contains: (1) a diagnostic item management table 71 for use to select diagnostic items unique to engine type according to the ECU code; (2) a vehicle diagnostic program storage area 72 for storing a vehicle diagnostic program related to a plurality of diagnostic items; (3) a standard data storage area 73 for storing standard data commonly used for a plurality types of the vehicles

irrespective of the type of the ECU mounted thereon; and (4) a unique data storage area 74 for storing unique data, the contents of which may vary according to each individual ECU. (Col. 5, lines 8-19). ROM 7 can store new or changed information, such as when a new car is introduced. ROM 7 can also store the vehicle diagnostic system and the information contained therein can be read into the CPU through the ROM card interface. (Col. 4, lines 50-58). *Sasaki* does not teach that the information from the ROM is downloaded into a storage device in the diagnostic tool. After diagnosis is completed, the operator then causes the vehicle diagnostic apparatus 2 to transmit the data on the diagnostic results of several vehicles from the transmitter 24 to a host machine, such as a host computer 30, which includes a mass storage device 33. (Col. 4, line 65 – Col. 5, line 3). In the host computer 30, a plurality of data sets, each representing the diagnostic results transferred in the plural data sets, are then incorporated into one unit and stored into the storage device 33. (Col. 15, lines 23-37). The transmission shown in Fig. 1 is unidirectional and no software is indicated as being transferred to the vehicle diagnostic apparatus 2 from the host computer. Thus, software can not be downloaded from a second storage device into the diagnostic tool or that the second storage device can transmit any security signature for that matter.

Chainer teaches an event recorder that attaches to a machine or vehicle, which can broadcast an encrypted signature, thereby leaving behind an electronic version of a "fingerprint" of the machine or vehicle carrying the recorder. The fingerprint, captured by an external data acquisition system, provides a history of events related to the machine or vehicle. The event recorder includes a microcomputer, a memory, and a transceiver that are preferably housed in a tamper resistant casing. The memory stored signature information about the vehicle, such as the owner's name, license plate, vehicle registration, etc. In a first mode of operation, monitoring

stations can periodically send an interrogation signal, such as when a radar gun detects that the vehicle is speeding. Upon receiving the interrogation signal, a smart card transmits the vehicle's signature information to the monitoring station where the time and date is stamped along with the speed of the vehicle. In a second mode of operation, when a sensor detects a sudden or violent acceleration or deceleration, such as during a collision, an event recorder mounted in each car will begin transmitting its signature information and receiving and storing the other vehicle's signature information. It is important that the smart card from, which signature data was received, can be authenticated to ensure that the signature data has not been altered. The smart cards can be authenticated, yet duplication resistant, by employing zero-knowledge protocols. Zero knowledge protocols allow a smart card 101 to be authenticated and yet be duplication resistant by allowing the verifying agent to convince him/herself that the smart card is authentic without the smart card revealing its authentication information. (Col. 3, lines 28-56). The actual security signature information is not exchanged or required to be the same in order for something to happen, such as allowing a software to download into a tool.

As shown above, the references alone or in combination do not disclose all the elements claimed invention, such as a method for preventing unauthorized downloading of software that includes at least providing a first external storage device that is electrically coupled to the diagnostic tool, the first external storage device including a first security signature, providing a second external storage device that is electrically coupled to the diagnostic tool, the second external storage device including software, and downloading the software into an internal storage device of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the first external storage device, as recited in claim 1. The references alone or combination also do not teach or suggest a diagnostic

tool that includes at least a first storage device including a first security signature, the second storage device including software, wherein the diagnostic tool downloads the software into a third storage device located within the diagnostic tool when a second security signature stored within the diagnostic tool is the same as the first security signature included within the first storage device, as recited in claim 11. The second external device (host computer 30 and data storage 33) can not transmit any software or a security signature to the diagnostic tool because the transmission of information as shown in FIG. 1 is from the diagnostic tool to the host computer and not vice versa. Additionally, the second external device does not contain a second security signature. There is no downloading of the software into the diagnostic tool when a second security signature is the same as the first security signature because the references use zero knowledge authentication protocols, which do not share authentication information. Additionally, no software download into a storage device in the diagnostic tool is taught by the references. Applicants respectfully request that the Examiner withdraw the rejection.

The references alone or combination do not teach or suggest a method for preventing unauthorized downloading of software that includes at least downloading the software into a memory of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the external storage device, as recited in claim 24. Additionally, the references alone or combination do not teach or suggest a diagnostic tool that includes at least the external storage device including a first security signature and software, where the diagnostic tool downloads the software into a memory of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the external storage device, as recited in claim 27. As stated above, the references do not disclose downloading software into a memory in the scan

tool or that the download occurs when a first and second security signature are the same. Applicants respectfully request that the Examiner withdraw the rejection.

Claims 8 and 18 include modifying the first security signature upon successful downloading of the software onto the internal storage device located within the diagnostic tool, while claims 9 and 19 further include the first security signature is modified so that it can not be further utilized to download the software into any diagnostic tool. *Arnold* (U.S. Patent No. 6,148,400) as stated by the Examiner deletes the private signature key after use. This of course, is not modifying the key because the key no longer exist, if it's deleted. Thus, *Sasaki* when combined with Arnold do not teach or suggest modifying the first signature after use.

Because claims 2-10; 12-23; 25, 26; and 28, 29 depend directly or indirectly from independent claims 1, 11, 24 and 27, respectively, that are believed to be in condition for allowance, these claims are also believed to be in condition for allowance. Withdrawal of the rejection is respectfully requested.

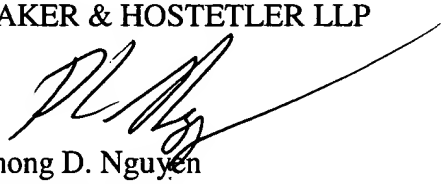
CONCLUSION

In view of the foregoing, it is respectfully submitted that the application is in condition for allowance. If it is believed that the application is not in condition for allowance the Examiner is requested to contact the undersigned attorney if it is believed that such contact will expedite the prosecution of the application.

In the event this paper is not timely filed, Applicants petition for an appropriate extension of time. Please charge any fee deficiencies or credit any overpayments to Deposit Account No. 50-2036.

Respectfully submitted,

BAKER & HOSTETLER LLP



Phong D. Nguyen
Reg. No. 43,833

Date: 6/30/09

Washington Square, Suite 1100
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5304
Telephone: 202-861-1500
Facsimile: 202-861-1783